NICHOLS ALGEBRAS OVER GROUPS WITH FINITE ROOT SYSTEM OF RANK TWO II

I. HECKENBERGER AND L. VENDRAMIN

Abstract. We classify all non-abelian groups G such that there exists a pair (V, W) of absolutely simple Yetter-Drinfeld modules over G such that the Nichols algebra of the direct sum of V and W is finite-dimensional under two assumptions: the square of the braiding between V and W is not the identity, and G is generated by the support of V and W. As a corollary, we prove that the dimensions of such V and W are at most six. As a tool we use the Weyl groupoid of (V, W).

Introduction

In the theory of Hopf algebras, deep structure results were achieved since the introduction of the Lifting Method of Andruskiewitsch and Schneider [5]. The aim of the method is to classify (finite-dimensional) pointed Hopf algebras. The idea of it is to generalize Lusztig's approach to quantum groups [19].

The Lifting Method is based on the understanding of the structure theory of certain braided Hopf algebras which are known as Nichols algebras. In Lusztig's setting this is the algebra $\mathbf{f}$, also known as $U_q(\mathfrak{n}_+)$. Motivated by the first classification results of finite-dimensional Nichols algebras of diagonal type [6][21], a complete solution was obtained by the first author [14]. The tool for the latter classification was the Weyl groupoid and the root system of a Nichols algebra of diagonal type, which was discovered in [13] using the theory of Lyndon words and PBW bases [18]. The Weyl groupoid was also used by Angiono to determine the defining relations of finite-dimensional Nichols algebras of diagonal type [8]. These results have far reaching consequences in the theory of Hopf algebras such as the classification of finite-dimensional pointed Hopf algebras with abelian coradical of order coprime to 210 [7], and the proof of the Andruskiewitsch-Schneider conjecture for pointed Hopf algebras with abelian coradical [9].

In order to understand the structure of Nichols algebras of non-diagonal type, the Weyl groupoid of a Nichols algebra of diagonal type was generalized further in several successive papers such as [4], [17], [16] and [15]. The first applications of this generalization were powerful enough to study pointed

István Heckenberger was supported by German Research Foundation via a Heisenberg professorship. Leandro Vendramin was supported by Conicet and the Alexander von Humboldt Foundation.

Hopf algebras in some cases where the coradical is a finite simple group [1, 2]. The difficulties towards extensions of these results and the scientific curiosity ask for a better understanding of finite-dimensional Nichols algebras of semisimple Yetter-Drinfeld modules over arbitrary groups.

In [15], H.-J. Schneider and the first author introduced a method to study the Weyl groupoid of a Nichols algebra over a Hopf algebra with invertible antipode. The main achievement of the paper was a description of $(\operatorname{ad} V)^n(W)$ for two Yetter-Drinfeld modules V, W in terms of the braiding. Also, a family $(G_n)_{n\geq 2}$ of groups was introduced as candidates admitting finite-dimensional Nichols algebras, and the finite-dimensional Nichols algebras over G_2 with finite root system of rank two were determined.

Roughly speaking, in this paper we prove that any non-abelian group G having a finite-dimensional Nichols algebra with an irreducible finite root system of rank two has to be a quotient of G_2, G_3, G_4 or another group T. As a corollary, we obtain that the dimension of the subspace of primitive elements of such a Nichols algebra has dimension at most 12. For the precise statement we refer to Theorem 4.5 and to Corollary 4.6. In order to obtain more precise claims on Nichols algebras over G, one has to perform detailed calculations about $(\operatorname{ad} V)^m(W)$ and $(\operatorname{ad} W)^m(V)$, $m \geq 1$, as in [15, §4].

Our method is based on the Weyl groupoid. Let V, W be absolutely simple Yetter-Drinfeld modules over G such that the pair (V, W) admits all reflections and the Weyl groupoid $\mathcal{W}(V, W)$ is finite. By [4, Thm. 3.12, Prop. 3.23], this is the case if the Nichols algebra of $V \oplus W$ is finite-dimensional. We prove that there exists an object of $\mathcal{W}(V, W)$ which has a Cartan matrix of finite type. Thus we have to analyze the consequences of $(\operatorname{ad} V)^2(W) = 0$, $(\operatorname{ad} W)^4(V) = 0$. We obtain restrictions regarding decomposability, size and further information on $\operatorname{supp} V$ and $\operatorname{supp} W$. In particular, Theorem 4.4 tells that for a pair (V, W) of Yetter-Drinfeld modules over G such that $(\operatorname{ad} V)(W) \neq 0$, $(\operatorname{ad} V)^2(W) = 0$ and $(\operatorname{ad} W)^4(V) = 0$ it is necessary that $\operatorname{supp} V \cup \operatorname{supp} W$ is isomorphic to one of five quandles, all of size at most six. Our results are based on Proposition 5.5 claiming the non-vanishing of $(\operatorname{ad} V)^{m+1}(W)$ under some assumptions on the structure of $\operatorname{supp} V$ and $\operatorname{supp} W$. It is an interesting fact that for this proposition and for many of its consequences we do not need to assume that V and W have finite support or that their supports are conjugacy classes!

The structure of the paper is as follows. First we recall some facts on groups with abelian centralizers, quandles and their enveloping groups in Sections 1 and 2. In Section 3 we prove with Corollary 3.2 that connected Weyl groupoids of rank two admitting a finite irreducible root system have an object with a Cartan matrix of finite type. Section 4 is devoted to the study of Nichols algebras over groups. After discussing some technicalities, we formulate our main results, Theorem 4.5 and Corollary 4.6. In Section 5 we give a step-by-step proof of Theorem 4.4.

1. Preliminaries

1.1. **Groups with abelian centralizers.** Recall from [20] that a group has *abelian centralizers* if the centralizer of every non-central element is abelian. The following definition goes back to Hall [12].

Definition 1.1. *Let G and H be two groups. We say that G is* isoclinic *to H if there exist isomorphisms $\zeta : G/Z(G) \to H/Z(H)$ and $\eta : [G,G] \to [H,H]$ such that if $g_1, g_2 \in G$, $h_1, h_2 \in H$, and $\zeta(g_i Z(G)) = h_i Z(H)$ for $i = 1, 2$, then $\eta[g_1, g_2] = [h_1, h_2]$. In this case we write $G \sim H$.*

It is clear that the relation of isoclinism is an equivalence relation. The following lemma is due to Hall [12, page 134].

Lemma 1.2. *Let G be a group and $K \lhd G$. The following hold.*

1. *$G/K \sim G/(K \cap [G,G])$.*
2. *If $K \subseteq [G,G]$ and $G \sim H$ for some group H via the maps ζ and η, then $\eta(K) \lhd H$ and $G/K \sim H/\eta(K)$.*

The following lemma was proved in [20, Lemma 3.4]. For completeness we give a proof in the context of this paper.

Lemma 1.3. *Let G and H be groups and assume $G \sim H$. If G has abelian centralizers, then H has abelian centralizers.*

Proof. Let $h \in H \setminus Z(H)$ and let $h_1, h_2 \in H^h$. Since $G \sim H$, there exist $g, g_1, g_2 \in G$ such that $\zeta(gZ(G)) = hZ(H)$ and $\zeta(g_i Z(G)) = h_i Z(H)$ for $i = 1, 2$. Further $g \notin Z(G)$ since $h \notin Z(H)$. Then $1 = [h, h_i] = \eta[g, g_i]$ and hence $g_i \in G^g$. Therefore $1 = \eta[g_1, g_2] = [h_1, h_2]$ and H^h is abelian. □

1.2. **Quandles.** Recall that a *quandle* is a non-empty set X with a binary operation $\triangleright$ such that the map $\varphi_i : X \to X$, $j \mapsto i \triangleright j$, is bijective for all $i \in X$, $i \triangleright (j \triangleright k) = (i \triangleright j) \triangleright (i \triangleright k)$ for all $i, j, k \in X$, and $i \triangleright i = i$ for all $i \in X$. The bijectivity of φ_i can be expressed by the existence of a map $\triangleleft : X \times X \to X$ such that $(i \triangleright j) \triangleleft i = j = i \triangleright (j \triangleleft i)$ for all $i, j \in X$. Then

$$k \triangleright (i \triangleleft j) = (k \triangleright i) \triangleleft (k \triangleright j), \quad (i \triangleleft j) \triangleleft k = (i \triangleleft k) \triangleleft (j \triangleleft k) \tag{1.1}$$

for all $i, j, k \in X$. A *crossed set* is a quandle X such that for all $i, j \in X$, $i \triangleright j = j$ implies $j \triangleright i = i$. Unions of conjugacy classes of a group with the binary operation of conjugation are examples of crossed sets.

Notation 1.4.

1. *To describe a finite quandle X we may assume that $X = \{1, \dots, n\}$ for some $n \in \mathbb{N}$ and then write $X : \varphi_1 \ \varphi_2 \ \cdots \ \varphi_n$ to denote the quandle structure on X given by $\varphi_1, \dots, \varphi_n$.*
2. *Let G be a group and $g \in G$. The quandle structure on the conjugacy class of g in G will be denoted by g^G.*

The *inner group* of a quandle X is the group $\mathrm{Inn}(X) = \langle \varphi_i : i \in X \rangle$ We say that a quandle X is *indecomposable* if the inner group $\mathrm{Inn}(X)$ acts transitively on X. Also, X is *decomposable* if it is not indecomposable.

Remark 1.5. Crossed sets of size at most three are well-known. If X is a crossed set and $1 \le |X| \le 2$ then X is trivial (or commutative), that is, $i \triangleright j = j$ for all $i, j \in X$. If $|X| = 3$ and X is non-trivial, then $i \triangleright j = k$ for all pairwise different elements $i, j, k \in X$. Hence $X \simeq (12)^{\mathbb{S}_3}$.

Remark 1.6. The classification (up to isomorphism) of indecomposable quandles of size ≤ 6 is well-known. The following is the list of such quandles:

$$\begin{aligned}
\{1\} &: \mathrm{id}\\
(12)^{\mathbb{S}_3} &: (23)\ (13)\ (12)\\
(123)^{\mathbb{A}_4} &: (243)\ (134)\ (142)\ (123)\\
\mathrm{Aff}(5,2) &: (2354)\ (1534)\ (1452)\ (1325)\ (1243)\\
\mathrm{Aff}(5,3) &: (2453)\ (1435)\ (1254)\ (1523)\ (1342)\\
\mathrm{Aff}(5,4) &: (25)(34)\ (13)(45)\ (15)(24)\ (12)(35)\ (14)(23)\\
(12)^{\mathbb{S}_4} &: (23)(56)\ (13)(45)\ (12)(46)\ (25)(36)\ (16)(24)\ (15)(34)\\
(1234)^{\mathbb{S}_4} &: (2436)\ (1654)\ (1456)\ (1253)\ (2634)\ (1352)
\end{aligned}$$

Let X be a quandle and let G_X denote its enveloping group

$$G_X = \langle x_i \,|\, i \in X\rangle / (x_i x_j = x_{i \triangleright j} x_i \text{ for all } i, j \in X).$$

This group is $\mathbb{Z}$-graded with $\deg(x_i) = 1$ for all $i \in X$.

Remark 1.7 (Universal property). For any group G and any map $f : X \to G$ satisfying $f(x \triangleright y) = f(x)f(y)f(x)^{-1}$ there exists a unique group homomorphism $g : G_X \to G$ such that $f = g \circ \partial$, where $\partial : X \to G_X$, $i \mapsto x_i$, see for example [3, Lemma 1.6].

Suppose that X is a finite indecomposable quandle. By [11, Lemmas 2.17 and 2.18], $x_i^{|\varphi_i|} = x_j^{|\varphi_j|}$ for all $i, j \in X$. This implies that the subgroup $K = \langle x_i^{|\varphi_i|} : i \in X\rangle$ is cyclic and central. The *finite enveloping group* is the finite group $\overline{G_X} = G_X / K$, see [11, Lemma 2.19]. Let $\pi : G_X \to \overline{G_X}$ be the canonical surjection.

A quandle X is *injective* if the map $\partial : X \to G_X$, $i \mapsto x_i$, is injective. For example, the group $\overline{G_X}$ can be used to test indecomposable quandles for injectivity.

Lemma 1.8. *Let X be a finite indecomposable quandle and let $u \in G_X$. Then the following hold.*

(1) *The restriction of π to the class u^{G_X} is a quandle isomorphism.*
(2) *X is injective if and only if $X \xrightarrow{\partial} G_X \xrightarrow{\pi} \overline{G_X}$ is injective.*

Proof. Let $v \in G_X$ and assume that u and v are conjugate. Then u and v have the same $\mathbb{Z}$-degree in G_X. Now, if $\pi u = \pi v$, then $u = v x_1^{m|\varphi_1|}$ for some $m \in \mathbb{Z}$. The $\mathbb{Z}$-graduation of G_X implies that $m = 0$ and hence $u = v$. Thus (1) is proved. Now (2) follows from (1). $\square$

Corollary 1.9. *Let X be a finite indecomposable quandle and*

$$M = \max\{|\mathcal{O}| : \mathcal{O} \text{ is a conjugacy class of } \overline{G_X}\}.$$

Then every conjugacy class of G_X has at most M elements.

Lemma 1.10. *Let X be a finite indecomposable quandle. Then $G_X \sim \overline{G_X}$.*

Proof. Let $\pi : G_X \to \overline{G_X}$ be the canonical surjection. Since the elements of $[G_X, G_X]$ have degree zero, $\ker \pi \cap [G_X, G_X] = \langle x_1^{|\varphi_1|} \rangle \cap [G_X, G_X] = 1$. Then the claim follows from Lemma 1.2(1) with $G = G_X$, $K = \ker \pi$. □

We conclude the subsection on quandles with two technical lemmas needed for the proof of our main result.

Lemma 1.11. *Let X be a crossed set, $Y \subseteq X$ a subset, and*

$$C(Y) = \{i \in X \,|\, \forall j \in Y : i \triangleright j = j\}.$$

Assume that $Y \cup C(Y) = X$. Then $X \triangleright Y = Y$.

Proof. Let $p, q \in C(Y)$ and $i \in Y$. Then

$$(p \triangleright q) \triangleright i = p \triangleright (q \triangleright i) = p \triangleright i = i$$

and hence $C(Y) \triangleright C(Y) \subseteq C(Y)$. Since $Y \triangleright C(Y) = C(Y)$ by definition of $C(Y)$ and since $X = Y \cup C(Y)$, we conclude that $X \triangleright C(Y) \subseteq C(Y)$. Since $i \triangleleft p = i \triangleleft q = i$, we obtain similarly that $C(Y) \triangleleft C(Y) \subseteq C(Y)$ and that $C(Y) \triangleleft X \subseteq C(Y)$. Hence $X \triangleright C(Y) = C(Y)$ and $X \triangleright (X \setminus C(Y)) = X \setminus C(Y)$.

Let $k \in Y \cap C(Y)$. Then $i \triangleright k = k$ for all $i \in Y$ since $k \in C(Y)$, and $i \triangleright k = k$ for all $i \in C(Y)$ since $k \in Y$. Since $Y \cup C(Y) = X$, we conclude that $X \triangleright \{k\} = \{k\}$ for all $k \in Y \cap C(Y)$. This and the first paragraph imply that $X \triangleright Y = Y$. □

Lemma 1.12. *Let $X = Y_1 \cup Y_2$ be a finite quandle, where Y_1 and Y_2 are disjoint $\mathrm{Inn}(X)$-orbits. Assume that there exists an isomorphism of quandles $g : Y_1 \to Y_2$ and that Y_1 is commutative. Then X is isomorphic to the quandle structure on $\{1, \dots, 2n\}$ given by*

$$\varphi_i = \begin{cases} (n+1 \ \cdots \ 2n) & \text{if } 1 \le i \le n, \\ (1 \ \cdots \ n) & \text{if } n+1 \le i \le 2n. \end{cases} \tag{1.2}$$

Proof. Without loss of generality we may assume that $Y_1 = \{1, \dots, n\}$ and $Y_2 = \{n+1, \dots, 2n\}$. For all $i \in Y_1$ and $j \in Y_2$ the permutations φ_i and φ_j commute, since $\operatorname{supp} \varphi_i \subseteq Y_2$ and $\operatorname{supp} \varphi_j \subseteq Y_1$. Further,

$$\varphi_{j \triangleright i} = \varphi_j \varphi_i \varphi_j^{-1} = \varphi_i.$$

As $\varphi_{k \triangleright i} = \varphi_i$ for all $k \in Y_1$ by the commutativity of Y_1, we conclude that $\varphi_i = \varphi_l$ for all $i, l \in Y_1$ since Y_1 is an $\mathrm{Inn}(X)$-orbit.

Since Y_1 and Y_2 are isomorphic, $\varphi_i = \varphi_l$ for all $i, l \in Y_2$. Since Y_1 is an $\mathrm{Inn}(X)$-orbit, it is a φ_{n+1}-orbit and hence for all $j \in Y_2$ the permutation φ_j is a cycle of length $|Y_1|$. This implies the claim. □

2. Groups with finite-dimensional Nichols algebras

Here we introduce the groups that realize the examples of decomposable quandles which are essential for our classification. These quandles are:

$$X_T^{4,1} : \ (243)\ (134)\ (142)\ (123)\ \mathrm{id}$$
$$X_2^{2,2} : \ (24)\ (13)\ (24)\ (13)$$
$$X_3^{3,1} : \ (23)\ (13)\ (12)\ \mathrm{id}$$
$$X_3^{3,2} : \ (23)(45)\ (13)(45)\ (12)(45)\ (123)\ (132)$$
$$X_4^{4,2} : \ (24)(56)\ (13)(56)\ (24)(56)\ (13)(56)\ (1234)\ (1432)$$

First we study the dimension of group representations.

Lemma 2.1. *Let G be a group, $x \in G$, and $d \in \mathbb{N}$. Suppose that $[G : G^x]$ is finite. If $\dim_{\mathbb{K}} V \leq d$ for any finite-dimensional absolutely simple $\mathbb{K}G^x$-module V, then $\dim_{\mathbb{K}} U \leq d[G : G^x]$ for any finite-dimensional absolutely simple $\mathbb{K}G$-module U. In particular, $\dim_{\mathbb{K}} U \leq [G : G^x]$ if G^x is abelian.*

Proof. We may assume that $\mathbb{K}$ is algebraically closed. Let U be a simple $\mathbb{K}G$-module with $\dim_{\mathbb{K}} U < \infty$ and let V be a simple $\mathbb{K}G^x$-submodule of U. Then $U = \mathbb{K}GV$ is an epimorphic image of $\mathbb{K}G \otimes_{\mathbb{K}G^x} V$ and $\dim_{\mathbb{K}} V \leq d$, and hence $\dim_{\mathbb{K}} U \leq d[G : G^x]$. Now the second claim follows, as finite-dimensional absolutely simple modules of abelian groups are one-dimensional. □

2.1. **The group T.**

Let us consider the group

$$T = \langle z \rangle \times \langle x_1, x_2, x_3, x_4 \mid x_i x_j = x_{\varphi_i(j)} x_i, \quad i, j \in \{1, 2, 3, 4\} \rangle,$$

where $\{\varphi_i : 1 \leq i \leq 4\}$ is the set of permutations that defines $(123)^{\mathbb{A}_4}$. This group is not nearly abelian, see [15, Definition 3.1], since the commutator subgroup $[T, T]$ is not cyclic. For example $[x_1, x_2]$ and $[x_1, x_3]$ do not commute. (One can prove that $[T, T] \simeq Q_8$, the quaternion group of eight elements.)

Example 2.2. Let $X_T^{4,1} = x_1^T \cup z^T$, see Notation 1.4(2). Then T is isomorphic to the enveloping group of $X_T^{4,1}$.

Lemma 2.3. *Let G be a quotient of T. Then the following hold.*

(1) *G has abelian centralizers.*
(2) *Every conjugacy class of G has at most six elements.*
(3) *Every finite-dimensional absolutely simple $\mathbb{K}G$-module has dimension at most four.*

Proof. By Lemma 1.3, we may replace G by a group which is isoclinic to G. Let $K \lhd T$ with $G = T/K$. By Lemma 1.2(1) we may assume that $K \subseteq [T, T]$. Let $X = (123)^{\mathbb{A}_4}$. Since $T \sim G_X$ and $G_X \sim \overline{G_X}$ by Lemma 1.10, $T/K \sim \overline{G_X}/L$ for some $L \lhd \overline{G_X}$ by Lemma 1.2(2). Now $\overline{G_X} \simeq \mathbf{SL}(2, 3)$ and

the only non-trivial normal subgroups of $\mathbf{SL}(2,3)$ are its commutator subgroup and its center. Since all quotients of $\mathbf{SL}(2,3)$ have abelian centralizers, Claim (1) holds.

To prove (2) we use Corollary 1.9, as every conjugacy class of $\mathbf{SL}(2,3)$ has at most six elements. Then Lemma 2.1 and (1) and $|X|=4$ imply (3). $\square$

2.2. **The groups G_n.** Let $n\in\mathbb{N}_{\geq 2}$. Recall from [15] that

$$G_n=\langle g,h,\epsilon \mid hg=\epsilon gh,\ g\epsilon=\epsilon^{-1}g,\ h\epsilon=\epsilon h,\ \epsilon^n=1\rangle.$$

Any element of G_n can be written uniquely as $\epsilon^i h^j g^k$, where $0\leq i\leq n-1$ and $j,k\in\mathbb{Z}$. By [15, §3], the conjugacy classes of G_n are

$$z^{G_n}=\{z\},\quad (gz)^{G_n}=\{\epsilon^m gz \mid 0\leq m\leq n-1\},$$
$$(h^jz)^{G_n}=\{h^jz,\epsilon^{-j}h^jz\},\quad (hgz)^{G_n}=\{\epsilon^m hgz \mid 0\leq m\leq n-1\},$$

where $z\in Z(G_n)=\langle \epsilon^{-1}h^2,h^n,g^2\rangle$ and $1\leq j\leq n/2$. The centralizers

$$(G_n)^{gz}=\langle \epsilon^{-1}h^2,g,h^n\rangle,\quad (G_n)^{hgz}=\langle \epsilon^{-1}h^2,hg,h^n\rangle,\quad (G_n)^{h^jz}=\langle \epsilon,h,g^2\rangle$$

are abelian. The commutator subgroup is $[G_n,G_n]=\langle\epsilon\rangle$.

Now we show four examples of decomposable quandles.

Example 2.4. Let $X_2^{2,2}=h^{G_2}\cup g^{G_2}$. Then $X_2^{2,2}\simeq\mathbb{D}_4$, the dihedral quandle of four elements. The enveloping group of $X_2^{2,2}$ is

$$\langle x_1,x_2,x_3,x_4 \mid x_ix_j=x_{2i-j\,(\mathrm{mod}\,4)}x_i,\ i,j\in\{1,2,3,4\}\rangle\simeq G_2.$$

The isomorphism is given by $x_1\mapsto g$, $x_2\mapsto h$.

Example 2.5. Let $X_3^{3,1}=g^{G_3}\cup\{\epsilon h\}$. Note that $\epsilon h\in Z(G_3)$. The enveloping group of $X_3^{3,1}$ is isomorphic to

$$\langle z\rangle\times\langle x_1,x_2,x_3 \mid x_ix_j=x_{2i-j\,(\mathrm{mod}\,3)}x_i,\ i,j\in\{1,2,3\}\rangle\simeq G_3.$$

The latter isomorphism is given by $z\mapsto\epsilon h$, $x_1\mapsto g$, $x_2\mapsto\epsilon g$ and $x_3\mapsto\epsilon^2 g$.

Example 2.6. Let $X_3^{3,2}=g^{G_3}\cup h^{G_3}$. The enveloping group of $X_3^{3,2}$ is isomorphic to G_3.

Example 2.7. Let $X_4^{4,2}=g^{G_4}\cup h^{G_4}$. The enveloping group of $X_4^{4,2}$ is isomorphic to G_4.

Lemma 2.8. *Let G be a quotient of G_n for some $n\geq 1$. Then the following hold.*

1. *G has abelian centralizers.*
2. *Every conjugacy class of G has at most four elements.*
3. *Every finite-dimensional absolutely simple $\mathbb{K}G$-module has dimension at most four.*

Proof. Let $p : G_n \to G$ be the canonical map. If $\epsilon^k \in \ker p$ for some $p > 0$, then G is also a quotient of G_k. Since $[G_n, G_n] = \langle \epsilon \rangle$, we may asume that $\ker p \cap [G_n, G_n] = 1$. Hence $G_n \sim G$ by Lemma 1.2(1). Therefore (1) follows from Lemma 1.3, since G_n has abelian centralizers.

Claim (2) follows from the description of conjugacy classes of G_n. Finally (3) follows from Lemma 2.1 and (1)–(2). □

3. Weyl groupoids of rank two

Let us consider the map

$$\eta : \mathbb{Z} \to \mathbf{SL}(2, \mathbb{Z}), \quad \eta(c) = \begin{pmatrix} c & -1 \\ 1 & 0 \end{pmatrix}.$$

A finite sequence $(c_1, c_2, \dots, c_n)$, $n \in \mathbb{N}$, of positive integers is a *characteristic sequence* if $\eta(c_1) \cdots \eta(c_n) = -\mathrm{id}$, and the entries of the first column of the matrix $\eta(c_1) \cdots \eta(c_i)$ are non-negative integers for all $i < n$. We denote by $\mathcal{A}^+$ the set of characteristic sequences. By [10, Lemma 5.2],

$$(c_1, c_2, \dots, c_n) \in \mathcal{A}^+, c_2 = 1, n \geq 4 \Leftrightarrow (c_1 - 1, c_3 - 1, c_4, \dots, c_n) \in \mathcal{A}^+. \tag{3.1}$$

Lemma 3.1. *Let $(c_1, c_2, \dots, c_n) \in \mathcal{A}^+$. Then $n \geq 3$ and there exists $i \in \{1, \dots, n\}$ such that $c_i = 1$ and $c_{i+1} \in \{1, 2, 3\}$, or $c_i = 1$ and $c_{i-1} \in \{1, 2, 3\}$, where $c_0 = c_n$ and $c_{n+1} = c_1$.*

Proof. Let $(c_1, c_2, \dots, c_n) \in \mathcal{A}^+$. If $n \leq 3$ then $(c_1, \dots, c_n) = (1, 1, 1)$ by [10, Prop. 5.3(4)]. Hence we may assume that $n > 3$. By [10, Cor. 4.2], there exists $i \in \{1, \dots, n\}$ such that $c_i = 1$. Further, $(c_j, c_{j+1}, \dots, c_n, c_1, \dots, c_{j-1}) \in \mathcal{A}^+$ for all $j \in \{1, \dots, n\}$ by [10, Prop. 5.3(2)]. Also, $c_i = 1$ implies that $c_{i-1}, c_{i+1} > 1$ by (3.1). Therefore, without loss of generality we may assume that $c = (b_1, b_2, \dots, b_r)$, where $b_i = (c_{i1}, 1, c_{i2}, 1, \dots, c_{im_i}, 1, c_{im_i+1})$ and $c_{ij} \geq 2$ for all $1 \leq i \leq r$, $1 \leq j \leq m_i + 1$, or $c = (d_1, 1, \dots, d_m, 1)$ with $n = 2m$, $d_1, \dots, d_m \geq 2$.

Assume first that $c = (b_1, b_2, \dots, b_r)$. Then $m_i \geq 2$ for at least one i. By applying (3.1) several times we obtain that $(b'_1, b'_2, \dots, b'_r) \in \mathcal{A}^+$, where

$$b'_i = (c_{i1} - 1, c_{i2} - 2, c_{i3} - 2, \dots, c_{im_i} - 2, c_{im_i+1} - 1) \quad \text{for all } 1 \leq i \leq r.$$

Since $(b'_1, b'_2, \dots, b'_r) \in \mathcal{A}^+$, by [10, Cor. 4.2] there exists $i \in \{1, \dots, r\}$ such that $c_{i1} - 1 = 1$ or $c_{im_i+1} - 1 = 1$ or $c_{ij} - 2 = 1$ for some $j \in \{2, \dots, m_i\}$. Then the lemma holds.

Now assume that $c = (d_1, 1, d_2, 1, \dots, d_m, 1)$, $n = 2m$. If $d_i = 2$ for some $1 \leq i \leq m$ then we are done. Otherwise, after applying (3.1) m times we obtain that $(d_1 - 2, d_2 - 2, \dots, d_m - 2) \in \mathcal{A}^+$. Hence there exists $i \in \{1, \dots, m\}$ such that $d_i - 2 = 1$. This implies the lemma. □

Cartan schemes of rank two, their Weyl groupoids and their root systems were studied in [10]. An indecomposable Cartan matrix $C \in \mathbb{Z}^{2\times 2}$ of finite

type is a matrix of the form

$$\begin{pmatrix} 2 & -c_1 \\ -c_2 & 2 \end{pmatrix},$$

where $c_1, c_2 \in \mathbb{N}$, $1 \le c_1 c_2 \le 3$.

Corollary 3.2. *Let $\mathcal{C} = \mathcal{C}(\{1,2\}, A, (\rho_i)_{i\in\{1,2\}}, (C^a)_{a\in A})$ be a connected Cartan scheme admitting a finite irreducible root system $(R^a)_{a\in A}$. Then there exists $a \in A$ such that $C^a \in \mathbb{Z}^{2\times 2}$ is an indecomposable Cartan matrix of finite type.*

Proof. Let $a \in A$, $n = |R^a_+|$, $a_1, \dots, a_{2n} \in A$, $c_1, \dots, c_{2n} \in \mathbb{N}$ such that

$$\begin{aligned} a_{2r-1} &= (\rho_2\rho_1)^{r-1}(a), & a_{2r} &= \rho_1(\rho_2\rho_1)^{r-1}(a), \\ c_{2r-1} &= -\, c_{12}^{a_{2r-1}}, & c_{2r} &= -\, c_{21}^{a_{2r}} \end{aligned}$$

for all $r \in \{1, 2, \dots, n\}$. Then $(c_1, \dots, c_n) \in \mathcal{A}^+$ by [10, Prop. 6.5]. By Lemma 3.1, there exists i such that $c_i = 1$ and $c_{i+1} \in \{1, 2, 3\}$, or $c_i = 1$ and $c_{i-1} \in \{1, 2, 3\}$. This implies the corollary. □

4. Nichols algebras over groups

Recall that a Yetter-Drinfeld module over a group G is a $\mathbb{K}G$-module $V = \oplus_{g\in G} V_g$ such that $hV_g \subseteq V_{hgh^{-1}}$ for all $g, h \in G$.

Lemma 4.1. *Let G be a quotient of one of the groups G_2, G_3, G_4 or T. Then every finite-dimensional absolutely simple Yetter-Drinfeld module over G has dimension at most six.*

Proof. Any simple Yetter-Drinfeld module over G is uniquely given by a conjugacy class $\mathcal{O}$ of G and an irreducible representation ρ of the centralizer of an element of $\mathcal{O}$. In this case, $\dim V = |\mathcal{O}| \deg \rho$. Hence the claim follows from Lemmas 2.8 and 2.3. □

For the study of Nichols algebras over groups the Weyl groupoid of a tuple of simple Yetter-Drinfeld modules plays an important role. For the definition we refer to [15].

Theorem 4.2. *Let $\theta \in \mathbb{N}$, let H be a Hopf algebra with bijective antipode and let $M = (M_1, \dots, M_\theta)$, where each M_i is a simple Yetter-Drinfeld module over H. Assume that M admits all reflections and that the Weyl groupoid $\mathcal{W}(M)$ is finite. Then $\mathfrak{B}(M)$ is decomposable and admits a finite root system of type $\mathcal{C}(M)$.*

Proof. By [15, Cor. 2.4], $\mathfrak{B}(M)$ is decomposable. Then the theorem becomes precisely [15, Thm. 2.3]. □

For any Yetter-Drinfeld module V over a Hopf algebra H with bijective antipode let $[V]$ denote the isomorphism class of V. The first step in the proof of Theorem 4.5 will be the following claim.

Proposition 4.3. *Let H be a Hopf algebra with bijective antipode and let $M = (M_1, M_2)$ be a pair of simple Yetter-Drinfeld modules over H. Assume that M admits all reflections and that $\mathcal{W}(M)$ is finite. Then there exists a pair $N = (N_1, N_2)$ of simple Yetter-Drinfeld modules over H, such that $[N] = ([N_1], [N_2]) \in \mathcal{W}(M)$ and $1 \le a_{12}^{[N]} a_{21}^{[N]} \le 3$.*

Proof. The claim follows from Corollary 3.2. □

Theorem 4.4. *Let $\mathbb{K}$ be a field, G be a non-abelian group, and V and W be two Yetter-Drinfeld modules over G. Assume that G is generated as a group by $\mathrm{supp}\,(V \oplus W)$, $\mathrm{supp}\, V$ and $\mathrm{supp}\, W$ are conjugacy classes of G, $(\mathrm{ad}\, V)^2(W) = 0$ and $(\mathrm{ad}\, W)^4(V) = 0$. If $(\mathrm{id} - c_{W,V} c_{V,W})(V \otimes W) \neq 0$ then $\mathrm{supp}\,(V \oplus W)$ is isomorphic to one of the quandles*

$$X_T^{4,1}, X_2^{2,2}, X_3^{3,1}, X_3^{3,2} \text{ and } X_4^{4,2},$$

and G is a quotient of the corresponding enveloping groups T, G_2, G_3, G_3 and G_4, respectively.

Before proving Theorem 4.4 we turn our attention to some consequences.

Theorem 4.5. *Let $\mathbb{K}$ be a field, G be a non-abelian group, and V and W be finite-dimensional absolutely simple Yetter-Drinfeld modules over G. Assume that G is generated by $\mathrm{supp}\,(V \oplus W)$, the pair (V, W) admits all reflections, and the Weyl groupoid of (V, W) is finite. If $(\mathrm{id} - c_{W,V} c_{V,W})(V \otimes W) \neq 0$, then G is a quotient of T or G_n for some $n \in \{2, 3, 4\}$. Moreover, $\dim V \le 6$ and $\dim W \le 6$.*

Proof. Proposition 4.3 implies that after changing the object of $\mathcal{W}(V, W)$, and possibly interchanging V and W, we may assume that $(\mathrm{ad}\, V)(W) \neq 0$, $(\mathrm{ad}\, V)^2(W) = 0$ and $(\mathrm{ad}\, W)^4(V) = 0$. Theorem 4.4 implies that the group G is a quotient of G_n for $n \in \{2, 3, 4\}$ or a quotient of T. After applying reflections to the pair (V, W) we obtain new pairs (V', W') of absolutely simple Yetter-Drinfeld modules over G. Thus the claim follows from Lemma 4.1. □

Corollary 4.6. *Let $\mathbb{K}$ be a field, G be a non-abelian group, and V and W be finite-dimensional absolutely simple Yetter-Drinfeld modules over G. Assume that G is generated by $\mathrm{supp}\,(V \oplus W)$ and $\mathfrak{B}(V \oplus W)$ is finite-dimensional. If $(\mathrm{id} - c_{W,V} c_{V,W})(V \otimes W) \neq 0$, then $\dim V \le 6$ and $\dim W \le 6$.*

Proof. Assume that $\mathfrak{B}(V \oplus W)$ is finite-dimensional. Then (V, W) admits all reflections by [4, Cor. 3.18] and the Weyl groupoid is finite by [4, Prop. 3.23]. So Theorem 4.5 applies. □

5. Proof of Theorem 4.4

The key of our proof is Proposition 5.5 which allows us to construct non-zero elements of $(\mathrm{ad}\, V)^m(W)$ for any two Yetter-Drinfeld modules V, W over a group G and for any $m \in \mathbb{N}$ under some assumption on G. Then we split our analysis into two parts depending on the question whether $\mathrm{supp}\, V$ and $\mathrm{supp}\, W$ commute. Finally, we prove Theorem 4.4 in §5.4.

In the whole section, let G be a non-abelian group and let $V=\oplus_{s\in G}V_s$ and $W=\oplus_{t\in G}W_t$ be Yetter-Drinfeld modules over G.

5.1. General considerations.

Lemma 5.1. *Let G be a group, and $g,h\in G$. Assume that G is generated by g^G and h^G. Then $G=AB$, where $A=\langle g^G\rangle$, $B=\langle h^G\rangle$, and*

$$AB=\{ab\mid a\in A,\ b\in B\}.$$

Proof. Let $r\in g^G$ and $s\in h^G$. Writing $sr=r(r^{-1}sr)$ we conclude that $g^Gh^G=h^Gg^G$. From this the claim follows. □

Recall that $S_n\in\mathrm{End}(V^{\otimes n})$, where $n\in\mathbb{N}$, denotes the quantum symmetrizer.

Lemma 5.2. [16, Prop. 6.5] *Let $n\in\mathbb{N}$. Then*

$$(\mathrm{ad}\,V)^n(W)\simeq(S_n\otimes\mathrm{id})T_n(V^{\otimes n}\otimes W),$$

where $T_n\in\mathrm{End}(V^{\otimes n}\otimes W)$ is defined by

$$T_n=(\mathrm{id}-c^2_{n,n+1}c_{n-1,n}\cdots c_{1,2})\cdots(\mathrm{id}-c^2_{n,n+1}c_{n-1,n})(\mathrm{id}-c^2_{n,n+1}).$$

Lemma 5.3. [15, Thm. 1.1] *Let $\varphi_0=0$, $X_0^{V,W}=W$, and*

$$\begin{aligned}\varphi_m&=\mathrm{id}-c_{V^{\otimes(m-1)}\otimes W,V}\,c_{V,V^{\otimes(m-1)}\otimes W}+(\mathrm{id}\otimes\varphi_{m-1})c_{1,2},\\ X_m^{V,W}&=\varphi_m(V\otimes X_{m-1})\end{aligned}$$

for all $m\ge 1$. Then

$$(S_{n+1}\otimes\mathrm{id}_W)T_{n+1}=\varphi_{n+1}(\mathrm{id}_V\otimes S_n\otimes\mathrm{id}_W)(\mathrm{id}_V\otimes T_n).$$

and $(\mathrm{ad}\,V)^n(W)\simeq X_n^{V,W}$ for all $n\in\mathbb{N}_0$.

Let $m\in\mathbb{N}_0$. Recall that an element of $V^{\otimes m}\otimes W$ has *degree* $(r_1,\dots,r_m,s)$, where $r_1,\dots,r_m,s\in G$, if it is contained in $V_{r_1}\otimes\cdots V_{r_m}\otimes W_s$.

Let $r_1,r_2,\dots,r_m\in\mathrm{supp}\,V$ and $s\in\mathrm{supp}\,W$, and write

$$Q_m(r_1,\dots,r_m,s)=(S_m\otimes\mathrm{id})T_m(V_{r_1}\otimes\cdots\otimes V_{r_m}\otimes W_s)\subseteq V^{\otimes m}\otimes W.$$

Although the vector space $V^{\otimes m}\otimes W$ is graded by $(\mathrm{supp}\,V)^m\times\mathrm{supp}\,W$, the subspace $Q_m(r_1,\dots,r_m,s)$ is usually not graded. For $t\in V^{\otimes m}\otimes W$ we write $\mathrm{supp}\,t$ for the set of $d\in(\mathrm{supp}\,V)^m\times\mathrm{supp}\,W$, such that the homogeneous component of t of degree d is non-zero. We let

$$\mathrm{supp}\,Q=\{\mathrm{supp}\,t\,|\,t\in Q\}$$

for all subspaces $Q\subseteq V^{\otimes m}\otimes W$.

Remark 5.4. Let $m\in\mathbb{N}$. By Lemma 5.2, $(\mathrm{ad}\,V)^m(W)=0$ if and only if $\mathrm{supp}\,Q_m(r_1,\dots,r_m,s)=0$ for all $r_1,\dots,r_m\in\mathrm{supp}\,V$, $s\in\mathrm{supp}\,W$.

Proposition 5.5. *Let $m \in \mathbb{N}_0$, $p_1, \dots, p_m, r_1, \dots, r_m \in \operatorname{supp} V$ and p_{m+1}, $s \in \operatorname{supp} W$ such that*

$$(p_1, \dots, p_m, p_{m+1}) \in \operatorname{supp} Q_m(r_1, \dots, r_m, s).$$

Let $p \in \operatorname{supp} V$ and $i \in \{1, \dots, m+1\}$ and assume that

$$p_i \triangleright p \neq p, \quad p_j \triangleright p = p \text{ for all } j \text{ with } i < j \leq m+1, \tag{5.1}$$

$$p \notin \{p_j \mid 1 \leq j \leq m\} \cup \{(p_{j+1}p_{j+2} \cdots p_{m+1})^{-1} \triangleright p_j \mid 1 \leq j < i\}. \tag{5.2}$$

Then $(p \triangleright p_1, \dots, p \triangleright p_{i-1}, p, p_i, \dots, p_m, p_{m+1}) \in \operatorname{supp} Q_{m+1}(p, r_1, \dots, r_m, s)$.

Proof. Let $t \in Q_m(r_1, \dots, r_m, s)$ and let $p \in \operatorname{supp} V$. By Lemma 5.3, $\varphi_{m+1}(v \otimes t) \in Q_{m+1}(p, r_1, \dots, r_m, s)$ for all $v \in V_p$. Moreover, $\varphi_{m+1}(v \otimes t)$ is a sum of non-zero homogeneous tensors of degrees

$$\begin{gathered} (p \triangleright p'_1, \dots, p \triangleright p'_{j-1}, p, p'_j, \dots, p'_m, p'_{m+1}), \\ (p \triangleright p'_1, \dots, p \triangleright p'_{j-1}, pp'_j \cdots p'_{m+1} \triangleright p, p \triangleright p'_j, \dots, p \triangleright p'_m, p \triangleright p'_{m+1}) \end{gathered} \tag{5.3}$$

with $1 \leq j \leq m+1$, where $(p'_1, \dots, p'_m, p'_{m+1}) \in \operatorname{supp} t$. By assumption on $p_1, \dots, p_m, p_{m+1}$, the tuple

$$(p \triangleright p_1, \dots, p \triangleright p_{i-1}, p, p_i, p_{i+1}, \dots, p_m, p_{m+1}) \tag{5.4}$$

appears among the degrees in (5.3). It suffices to show that it appears exactly once. We split the proof into several cases.

Assume first that (5.4) is equal to $(p \triangleright p'_1, \dots, p \triangleright p'_{j-1}, p, p'_j, \dots, p'_m, p'_{m+1})$ for some $j \in \{1, \dots, m+1\}$. There are three cases to consider. First, if $j < i$, then $p \triangleright p_j = p$ and hence $p = p_j$, a contradiction to (5.2). If $j = i$ then we obtain $p_l = p'_l$ for all $l \in \{1, \dots, m+1\}$ which gives us just the tuple we are looking at. Finally, if $j > i$, then $p = p_{j-1}$, again a contradiction to (5.2).

Now assume that (5.4) is equal to

$$(p \triangleright p'_1, \dots, p \triangleright p'_{j-1}, pp'_j \cdots p'_{m+1} \triangleright p, p \triangleright p'_j, \dots, p \triangleright p'_m, p \triangleright p'_{m+1}) \tag{5.5}$$

for some $j \in \{1, \dots, m+1\}$. Again there are three cases to consider.

If $j > i$ then

$$p \triangleright p'_k = p_k \text{ for all } k \in \{j, j+1, \dots, m+1\}, \quad pp'_j \cdots p'_{m+1} \triangleright p = p_{j-1}.$$

By (5.1) we conclude that $p'_k = p_k$ for all $k \in \{j, j+1, \dots, m+1\}$ and $p = p_{j-1}$.

If $j = i$ then

$$p \triangleright p'_k = p_k \text{ for all } k \in \{i, i+1, \dots, m+1\}, \quad pp'_i \cdots p'_{m+1} \triangleright p = p.$$

We conclude from (5.1) that $p'_k = p_k$ for all $k \in \{i+1, \dots, m+1\}$, $p \triangleright p'_i = p_i$ and $pp'_i \triangleright p = p$. This implies that

$$p_i \triangleright p = (p \triangleright p'_i) \triangleright p = pp'_i p^{-1} \triangleright p = pp'_i \triangleright p = p,$$

a contradiction to (5.1).

Finally, assume that $1 \le j < i$. Then $pp'_j \cdots p'_{m+1} \triangleright p = p \triangleright p_j$, or

$$(p \triangleright p'_j)(p \triangleright p'_{j+1}) \cdots (p \triangleright p'_{m+1}) \triangleright p = p \triangleright p_j.$$

We conclude from this and the equality of (5.4) and (5.5) that

$$(p \triangleright p_{j+1}) \cdots (p \triangleright p_{i-1}) p p_i \cdots p_{m+1} \triangleright p = p \triangleright p_j.$$

The latter is equivalent to

$$p p_{j+1} \cdots p_{i-1} p_i \cdots p_{m+1} \triangleright p = p \triangleright p_j,$$

which after cancelling $p \triangleright$ gives a contradiction to (5.2). □

Remark 5.6. If $m = 0$ then Proposition 5.5 reads as follows. Let $s \in \operatorname{supp} W$ and $p \in \operatorname{supp} V$ and assume that $s \triangleright p \ne p$. Then $(p, s) \in \operatorname{supp} Q_1(p, s)$.

Corollary 5.7. *Let $m \ge 1$. Assume that the following hold.*

1. $\operatorname{supp} V$ *is indecomposable or* $\operatorname{supp} V = Y_1 \cup Y_2$ *is a decomposition into* $\operatorname{Inn}(\operatorname{supp} V)$*-orbits, and $x \triangleright Y_1 = Y_2$, $x \triangleright Y_2 = Y_1$ for all $x \in \operatorname{supp} W$.*
2. $(\operatorname{ad} V)^m(W) \ne 0$, $(\operatorname{ad} V)^{m+1}(W) = 0$.

Then $|\operatorname{supp} V| \le 2m - 1$ *if* $\operatorname{supp} V$ *and* $\operatorname{supp} W$ *commute, and* $|\operatorname{supp} V| \le 2m$ *otherwise.*

Proof. By (2), there exist $r_1, \dots, r_m, p_1 \dots, p_m \in \operatorname{supp} V$, $s', p_{m+1} \in \operatorname{supp} W$ and $t \in Q_m(r_1, \dots, r_m, s')$ such that $(p_1, \dots, p_{m+1}) \in \operatorname{supp} t$ and $\varphi_{m+1}(v \otimes t) = 0$ for all $p \in \operatorname{supp} V$, $v \in V_p$. Let

$$Y = \{p_j \mid 1 \le j \le m\} \cup \{(p_{j+1} p_{j+2} \cdots p_{m+1})^{-1} \triangleright p_j \mid 1 \le j \le m\}.$$

Then $|Y| \le 2m$. Moreover, if $r \triangleright s = s$ for all $r \in \operatorname{supp} V$, $s \in \operatorname{supp} W$, then $p_{m+1}^{-1} \triangleright p_m = p_m$ and hence $|Y| \le 2m - 1$. Therefore it suffices to prove that $Y = \operatorname{supp} V$.

By Proposition 5.5, any $p \in \operatorname{supp} V$ with $p \notin Y$ satisfies $p_j \triangleright p = p$ for all $j \in \{1, \dots, m+1\}$ and hence $\operatorname{supp} V = Y \cup C(Y)$. By Lemma 1.11, Y is $\operatorname{Inn}(\operatorname{supp} V)$-invariant. Thus $Y = \operatorname{supp} V$ if $\operatorname{supp} V$ is indecomposable. If $\operatorname{supp} V$ is decomposable as in (1), then p_m and $p_{m+1}^{-1} \triangleright p_m$ are in different components of $\operatorname{supp} V$ by (1). Therefore the $\operatorname{Inn}(\operatorname{supp} V)$-invariance of Y implies again that $Y = \operatorname{supp} V$. □

Corollary 5.8. *Let $r_1, r_2, r_3, r_4 \in \operatorname{supp} V$ and $s \in \operatorname{supp} W$. Assume that* $\operatorname{supp} V$ *and* $\operatorname{supp} W$ *commute, $(r_3, r_4, s) \in \operatorname{supp} Q_2(r_3, r_4, s)$, and*

$$r_2 \notin \{r_3, r_4, r_4^{-1} \triangleright r_3\}, \quad r_2 \triangleright r_4 \ne r_4, \tag{5.6}$$

$$r_1 \notin \{r_2 \triangleright r_3, r_2, r_4, r_4^{-1} \triangleright r_2, r_4^{-1} \triangleright r_3\}, \quad r_1 \triangleright r_4 \ne r_4. \tag{5.7}$$

Then $(\operatorname{ad} V)^4(W) \ne 0$.

Proof. Let $(p_1, p_2, p_3) = (r_3, r_4, s) \in \operatorname{supp} Q_2(r_3, r_4, s)$. By assumption, Conditions (5.1), (5.2) with $m = i = 2$, $p = r_2$ are fulfilled: $r_4 \triangleright r_2 \ne r_2$, $s \triangleright r_2 = r_2$ and $r_2 \notin \{r_3, r_4, r_4^{-1} \triangleright r_3\}$. Hence $(r_2 \triangleright r_3, r_2, r_4, s) \in \operatorname{supp} Q_3(r_2, r_3, r_4, s)$ by Proposition 5.5.

Now let $(p_1,p_2,p_3,p_4)=(r_2\triangleright r_3,r_2,r_4,s)\in \operatorname{supp} Q_3(r_2,r_3,r_4,s)$. Then

$$(p_3p_4)^{-1}\triangleright p_2=r_4^{-1}\triangleright r_2,\quad (p_2p_3p_4)^{-1}\triangleright p_1=r_4^{-1}\triangleright r_3.$$

By assumption, Conditions (5.1), (5.2) with $m=i=3$, $p=r_1$ are fulfilled: $p_3\triangleright p\neq p$, $p_4\triangleright p=p$, and $p\notin\{p_1,p_2,p_3,(p_3p_4)^{-1}\triangleright p_2,(p_2p_3p_4)^{-1}\triangleright p_1\}$. Hence $(r_1r_2\triangleright r_3,r_1\triangleright r_2,r_1,r_4,s)\in\operatorname{supp} Q_4(r_1,r_2,r_3,r_4,s)$ and therefore $(\operatorname{ad} V)^4(W)\neq 0$ by Remark 5.4. □

Corollary 5.9. *Assume that* $|\operatorname{supp} V|\geq 5$, $\operatorname{supp} V$ *and* $\operatorname{supp} W$ *commute,* $(\operatorname{ad} V)(W)\neq 0$ *and* $x\triangleright y\neq y$ *for all* $x,y\in\operatorname{supp} V$. *Then* $(\operatorname{ad} V)^4(W)\neq 0$.

Proof. Since $(\operatorname{ad} V)(W)\neq 0$, there exist $r_4\in\operatorname{supp} V$, $s\in\operatorname{supp} W$ with $Q_1(r_4,s)\neq 0$. Then $(r_4,s)=\operatorname{supp} Q_1(r_4,s)$. Let $r_3\in\operatorname{supp} V\setminus\{r_4\}$. Then $r_3\triangleright r_4\neq r_4$ and hence $(r_3,r_4,s)\in\operatorname{supp} Q_2(r_3,r_4,s)$ by Proposition 5.5. Since $|\operatorname{supp} V|\geq 5$, there exists $r_2\in\operatorname{supp} V$ with $r_2\notin\{r_3,r_4,r_4^{-1}\triangleright r_3,r_4\triangleright r_3\}$. By assumption, $r_2\triangleright r_4\neq r_4$. By construction,

$$r_3\notin\{r_2\triangleright r_3,r_2,r_4,r_4^{-1}\triangleright r_2,r_4^{-1}\triangleright r_3\},\quad r_3\triangleright r_4\neq r_4.$$

Thus Corollary 5.8 with $r_1=r_3$ implies that $(\operatorname{ad} V)^4(W)\neq 0$. □

Corollary 5.10. *Let* $r_1,r_2,r_3\in\operatorname{supp} V$ *and* $s\in\operatorname{supp} W$. *Assume that the following hold:*

(1) $r_2\triangleright r_3\neq r_3$,
(2) $r_1\notin\{r_3r_2\triangleright r_3,r_3\triangleright r_2,r_3,s^{-1}\triangleright r_3,s^{-1}\triangleright r_2\}$,
(3) $s\triangleright r_2,s\triangleright r_3\notin\{r_2,r_3\}$,
(4) $r_1\triangleright s\neq s$ *or* $r_1\triangleright r_3\neq r_3$.

Then $(\operatorname{ad} V)^4(W)\neq 0$.

Proof. Let $(p_1,p_2)=(r_3,s)$. Then $(p_1,p_2)\in\operatorname{supp} Q_1(r_3,s)$ since $s\triangleright r_3\neq r_3$. Conditions (5.1) and (5.2) with $m=1$, $i=2$ and $p=r_2$ are fulfilled: $p_2\triangleright p\neq p$, $p=r_2\notin\{r_3,s^{-1}\triangleright r_3\}$. Thus

$$(r_2\triangleright r_3,r_2,s)\in\operatorname{supp} Q_2(r_2,r_3,s)$$

by Proposition 5.5.

Let now $(p_1,p_2,p_3)=(r_2\triangleright r_3,r_2,s)\in\operatorname{supp} Q_2(r_2,r_3,s)$. Then Conditions (5.1) and (5.2) with $m=2$, $i=3$ and $p=r_3$ are fulfilled: $s\triangleright p\neq p$,

$$r_3\notin\{p_1,p_2,p_3^{-1}\triangleright p_2,(p_2p_3)^{-1}\triangleright p_1\}=\{r_2\triangleright r_3,r_2,s^{-1}\triangleright r_2,s^{-1}\triangleright r_3\}.$$

Hence $(r_3r_2\triangleright r_3,r_3\triangleright r_2,r_3,s)\in\operatorname{supp} Q_3(r_3,r_2,r_3,s)$ by Proposition 5.5.

Finally, let $(p_1,p_2,p_3,p_4)=(r_3r_2\triangleright r_3,r_3\triangleright r_2,r_3,s)\in\operatorname{supp} Q_3(r_3,r_2,r_3,s)$ and let $p=r_1$. Then

$$p_4^{-1}\triangleright p_3=s^{-1}\triangleright r_3,\ (p_3p_4)^{-1}\triangleright p_2=s^{-1}\triangleright r_2,\ (p_2p_3p_4)^{-1}\triangleright p_1=s^{-1}\triangleright r_3$$

and hence $p\notin\{p_1,p_2,p_3,p_4^{-1}\triangleright p_3,(p_3p_4)^{-1}\triangleright p_2,(p_2p_3p_4)^{-1}\triangleright p_1\}$. Since $p_4\triangleright p\neq p$ or $p_3\triangleright p\neq p$ by (4), Proposition 5.5 with $m=3$ implies that $Q_4(r_1,r_3,r_2,r_3,s)\neq 0$. Hence $(\operatorname{ad} V)^4(W)\neq 0$ by Lemma 5.2. □

Corollary 5.11. *Assume that* $\operatorname{supp} V$ *is an indecomposable quandle and that* $(\operatorname{ad} V)(W) \neq 0$*,* $(\operatorname{ad} V)^4(W) = 0$*. Then* $\operatorname{supp} V$ *is isomorphic to one of the quandles*

$$\{1\}, (12)^{\mathbb{S}_3}, (12)^{\mathbb{S}_4}, (123)^{\mathbb{A}_4}, \mathrm{Aff}(5,2), \mathrm{Aff}(5,3), \mathrm{Aff}(5,4), (1234)^{\mathbb{S}_4}. \tag{5.8}$$

Proof. Corollary 5.7 yields that $|\operatorname{supp} V| \le 6$ and Remark 1.6 applies. □

5.2. **Commuting supports.** Let $g, h \in G$. Assume that $\operatorname{supp} V = g^G$, $\operatorname{supp} W = h^G$, $G = \langle g^G \cup h^G \rangle$ and that g^G and h^G commute. We conclude an implication of $(\operatorname{ad} V)^2(W) = 0$, $(\operatorname{ad} W)^4(V) = 0$ on V and W.

Lemma 5.12. *The quandles* g^G *and* h^G *are indecomposable.*

Proof. It is sufficient to prove the claim on h^G. By Lemma 5.1 and since g^G and h^G commute, we obtain that

$$h^G = G \triangleright h = \langle h^G \rangle \langle g^G \rangle \triangleright h = \langle h^G \rangle \triangleright h = \mathrm{Inn}(h^G) \triangleright h.$$

Thus h^G is indecomposable. □

Lemma 5.13. *Assume that* $(\operatorname{ad} V)(W) \neq 0$ *and* $(\operatorname{ad} V)^2(W) = 0$*. Then* $g^G = \{g\}$*.*

Proof. This follows from Corollary 5.7 with $m = 1$ using Lemma 5.12. □

Proposition 5.14. *Assume that* $(\operatorname{ad} V)(W) \neq 0$*,* $(\operatorname{ad} V)^2(W) = 0$*, and* $(\operatorname{ad} W)^4(V) = 0$*. Then* $g^G \cup h^G$ *is isomorphic to* $X_3^{3,1}$ *or* $X_T^{4,1}$*.*

Proof. First, $g^G = \{g\}$ by Lemma 5.13. Further, h^G is indecomposable by Lemma 5.12. and $|h^G| \ge 2$ since $G = \langle g^G \cup h^G \rangle$ is non-abelian. Corollary 5.7 implies that $|h^G| \le 5$. Thus, by Corollary 5.11, h^G is isomorphic to one of the quandles $(12)^{\mathbb{S}_3}$, $(123)^{\mathbb{A}_4}$, $\mathrm{Aff}(5,2)$, $\mathrm{Aff}(5,3)$, $\mathrm{Aff}(5,4)$. Assume that h^G is one of the quandles $\mathrm{Aff}(5,2)$, $\mathrm{Aff}(5,3)$, $\mathrm{Aff}(5,4)$. Then $|h^G| = 5$ and $x \triangleright y \neq y$ for any $x, y \in h^G$ with $x \neq y$. Thus $(\operatorname{ad} W)^4(V) \neq 0$ by Corollary 5.9 and the proposition follows. □

5.3. **Non-commuting supports.** In this subsection let $g, h \in G$. Assume that $gh \neq hg$, $\operatorname{supp} V = g^G$, $\operatorname{supp} W = h^G$, and $G = \langle g^G \cup h^G \rangle$. Then for all $s \in h^G$ there exists $r \in g^G$ with $rs \neq sr$. We determine consequences of the equations $(\operatorname{ad} V)^2(W) = 0$ and $(\operatorname{ad} W)^4(V) = 0$.

Lemma 5.15. *Assume that* $(\operatorname{ad} V)^2(W) = 0$*. Then the following hold.*

(1) g^G *is commutative.*
(2) $g^G \neq h^G$.
(3) $g^G = \langle h^G \rangle \triangleright g$.
(4) *Let* $s \in h^G$*. Then there exist* $r_1, r_2 \in g^G$ *such that* $\varphi_s|_{g^G} = (r_1\, r_2)$*.*
(5) $h^2 \triangleright g = g$ *and* $(gh)^2 = (hg)^2$*.*
(6) *For all* $m \in \mathbb{Z}$*,* $\{x \in g^G \mid x \triangleright (g^m \triangleright h) \neq g^m \triangleright h\} = \{g, h \triangleright g\}$*.*

Proof. (4) and (1). First, $|g^G| \geq 2$ and $|h^G| \geq 2$ since $gh \neq hg$. Let $r_1 \in g^G$ and $s \in h^G$ such that $s \triangleright r_1 \neq r_1$. Then $(r_1, s) \in \operatorname{supp} Q_1(r_1, s)$ by Remark 5.6. Let $p \in g^G$. Assume that $p \notin \{r_1, s^{-1} \triangleright r_1\}$. Since $Q_2(p, r_1, s) = 0$ because of $(\operatorname{ad} V)^2(W) = 0$, Proposition 5.5 implies that $s \triangleright p = p = r_1 \triangleright p$. Then $\varphi_s|_{g^G} = (r_1\, s^{-1} \triangleright r_1)$ which is the claim in (4). The equation $r_1 \triangleright p = p$ implies that $r_1 \triangleright r_2 = r_2$ for all $r_2 \in g^G$. Thus (1) holds.

(2). If $g^G = h^G$ then $G = \langle g^G \rangle$ is commutative by (1), a contradiction.

(3). Lemma 5.1 and (1) yield that $g^G = G \triangleright g = \langle h^G \rangle \langle g^G \rangle \triangleright g = \langle h^G \rangle \triangleright g$.

(5). From (1) we know that $g \triangleright (h \triangleright g) = h \triangleright g$ and hence $hgh \triangleright g = h^2 \triangleright g = g$, where the second equation follows from (4). This implies (5).

(6). By (1), g^G is commutative. Thus it suffices to prove the claim for $m = 0$. The latter follows from (4) with $s = h$ since $gh \neq hg$. □

Lemma 5.16. *Assume that* $(\operatorname{ad} V)^2(W) = 0$ *and that* h *commutes with* $g \triangleright h$. *Then the following hold.*

(1) *For all* $m \in \mathbb{Z}$, $(h \triangleright g) \triangleright (g^m \triangleright h) = g^{m+1} \triangleright h$.
(2) $\langle g^G \rangle \triangleright h = \langle g \rangle \triangleright h$.

Proof. First we prove (1). By Lemma 5.15(1), g^G is commutative. Thus it suffices to consider the case $m = 0$. Now $(h \triangleright g) \triangleright h = hg \triangleright h = g \triangleright h$ by assumption.

Now we prove (2). Lemma 5.15(4) and (1) with $m \in \{-1, 0\}$, imply that

$$(g^G)^{\pm 1} \triangleright h \subseteq \{h\} \cup \{g, g^{-1}, h \triangleright g, (h \triangleright g)^{-1}\} \triangleright h \subseteq \{h, g \triangleright h, g^{-1} \triangleright h\}.$$

Now write $\langle g^G \rangle = \cup_{m \in \mathbb{N}_0} A_m$, where $A_m = \{x_1^{\pm 1} \cdots x_m^{\pm 1} \mid x_i \in g^G\}$. It suffices to show that $A_m \triangleright h \subseteq \langle g \rangle \triangleright h$ for all $m \in \mathbb{N}_0$. We proceed by induction on m. The case $m = 0$ is trivial and the case $m = 1$ was just proven. Let now $m \in \mathbb{N}$ and assume that $A_m \triangleright h \subseteq \langle g \rangle \triangleright h$. Using the induction hypothesis and the fact that g^G is commutative, see Lemma 5.15(1), we obtain that

$$\begin{aligned} A_{m+1} \triangleright h &= (g^G)^{\pm 1} \triangleright (A_m \triangleright h) \\ &\subseteq (g^G)^{\pm 1} \triangleright (\langle g \rangle \triangleright h) = \langle g \rangle \triangleright ((g^G)^{\pm 1} \triangleright h) \subseteq \langle g \rangle \triangleright h. \end{aligned}$$

This implies (2). □

Lemma 5.17. *Assume that* $(\operatorname{ad} V)^2(W) = 0$ *and that* h^G *is commutative. Then* $g^G \cup h^G$ *is isomorphic to* $X_2^{2,2}$.

Proof. Lemma 5.15(4) implies that $ghg \triangleright h = h$. Since h^G is commutative, $hg \triangleright h = g \triangleright h$ and hence $h = ghg \triangleright h = g^2 \triangleright h$. Therefore

$$h^G = \langle g^G \rangle \langle h^G \rangle \triangleright h = \langle g^G \rangle \triangleright h = \{h, g \triangleright h\}$$

by Lemmas 5.1 and 5.16(2) and since h^G is commutative. Recall that g^G is commutative by Lemma 5.15(1) and that $h^2 \triangleright g = g$ by Lemma 5.15(5). From Lemma 5.1 we obtain

$$g^G = \langle h^G \rangle \langle g^G \rangle \triangleright g = \langle h^G \rangle \triangleright g = \langle h, g \triangleright h \rangle \triangleright g \subseteq \langle g, h \rangle \triangleright g = \{h \triangleright g, g\}.$$

Therefore $g^G = \{h \triangleright g, g\}$ and $g^G \cup h^G \simeq X_2^{2,2}$ as quandles. □

Lemma 5.18. *Let $x,y\in h^G$ such that $x\triangleright y=y$. Assume that $y\triangleright z\neq z$ for all $z\in h^G\setminus\{x,y\}$, and that $\varphi_x|_{g^G}=(r\,s)$ for some $r,s\in g^G$, $r\neq s$. Then $\varphi_y|_{g^G}=(r\,s)$.*

Proof. Since $x,y\in h^G$ and $\varphi_x|_{g^G}=(r\,s)$, there exist $a,b\in g^G$ such that $\varphi_y|_{g^G}=(a\,b)$. Assume that $(a\,b)\neq(r\,s)$. Then $|\{r,s,a,b\}|=4$ since $\varphi_x|_{g^G}$ and $\varphi_y|_{g^G}$ commute. Let $z=r\triangleright x$. First, $z=r\triangleright x\neq x$ since $x\triangleright r\neq r$. Second, $r\triangleright x\neq y$ since $\varphi_z|_{g^G}=(r\;r\triangleright s)\neq(a\,b)$. Hence $y\triangleright z\neq z$ by assumption, a contradiction to $y\triangleright(r\triangleright x)=(y\triangleright r)\triangleright(y\triangleright x)=r\triangleright x$. □

Lemma 5.19. *Let $x,y\in h^G$, $\psi_x=\varphi_x|_{g^G}$ and $\psi_y=\varphi_y|_{g^G}$. Assume that $(\operatorname{ad}V)^2(W)=0$ and that x,y generate the quandle h^G. If $\psi_x=\psi_y$ then $|g^G|=2$. Otherwise $|g^G|=3$ and $\psi_x\psi_y\neq\psi_y\psi_x$.*

Proof. By Lemma 5.15(1) and (4), g^G is commutative and there exist $g_1,g_2\in g^G$ such that $\psi_x=(g_1\;x\triangleright g_1)$ and $\psi_y=(g_2\;y\triangleright g_2)$. Assume now that $|\{g_1,x\triangleright g_1,g_2,y\triangleright g_2\}|=4$. Then $|g^G|\geq 4$. On the other hand, Lemma 5.1 and the commutativity of g^G imply that

$$g^G=G\triangleright g_1=\langle h^G\rangle\langle g^G\rangle\triangleright g_1=\langle h^G\rangle\triangleright g_1=\langle x,y\rangle\triangleright g_1=\{g_1,x\triangleright g_1\},\tag{5.9}$$

a contradiction to $|g^G|\geq 4$. Hence $|\{g_1,x\triangleright g_1,g_2,y\triangleright g_2\}|\leq 3$ and the lemma follows by two calculations similar to (5.9). □

Lemma 5.20. *Assume that $(\operatorname{ad}V)^2(W)=0$, h^G is decomposable and let $h^G=Y_1\cup\cdots\cup Y_k$ be the decomposition of h^G into orbits of the inner group of h^G. Then $k=2$ and $x\triangleright Y_1=Y_2$, $x\triangleright Y_2=Y_1$ for all $x\in g^G$.*

Proof. First, $h^G=g\triangleright h^G=(g\triangleright Y_1)\cup\cdots\cup(g\triangleright Y_k)$ is a decomposition into $\operatorname{Inn}(h^G)$-orbits: $(g\triangleright y)\triangleright(g\triangleright Y_i)=g\triangleright(y\triangleright Y_i)=g\triangleright Y_i$ for all $y\in h^G$, $1\leq i\leq k$. Thus φ_g permutes the orbits $Y_1,\dots,Y_k$. Since $g^G=\langle h^G\rangle\triangleright g$ by Lemma 5.15(3), each $x\in g^G$ permutes the $\operatorname{Inn}(h^G)$-orbits $Y_1,\dots,Y_k$ in the same way as g does. Let $Y\subset h^G$ be the $\operatorname{Inn}(h^G)$-orbit of h. As G is generated by $g^G\cup h^G$ and h^G is a conjugacy class of G, we conclude that

$$h^G=Y\cup(g\triangleright Y)\cup\cdots\cup(g^{k-1}\triangleright Y).$$

By Lemma 5.15(5), $ghg\triangleright h=h$ and hence $h\in Y\cap(g^2\triangleright Y)$. Thus $g^2\triangleright Y=Y$ and hence $h^G=Y\cup(g\triangleright Y)$ since h^G is decomposable. □

Lemma 5.21. *Assume that $(\operatorname{ad}V)^2(W)=0$, $(\operatorname{ad}W)^4(V)=0$ and that h^G is decomposable. Then $g^G\cup h^G$ is isomorphic to $X_2^{2,2}$ or to $X_4^{4,2}$.*

Proof. By Lemma 5.20, $h^G=Y_1\cup Y_2$, where Y_1 and Y_2 are the $\operatorname{Inn}(h^G)$-orbits of h^G. Moreover, $x\triangleright Y_1=Y_2$ and $x\triangleright Y_2=Y_1$ for all $x\in g^G$. Thus Corollary 5.7 implies that $|h^G|\leq 6$. There are two cases to consider.

Assume first that Y_1 is non-commutative. Then $Y_1\simeq Y_2\simeq(12)^{\mathbb{S}_3}$ by Remark 1.5. Let $r_3\in Y_1$, $r_2\in Y_1\setminus\{r_3\}$ and $r_1\in Y_2\setminus\{g^{-1}\triangleright r_3,g^{-1}\triangleright r_2\}$. By Corollary 5.10 with $s=g$, $(\operatorname{ad}W)^4(V)\neq 0$, a contradiction.

Assume now that Y_1 is commutative. By Lemma 1.12, the permutations φ_i defining h^G are given by (1.2). Further, $x \triangleright y \neq y$ and hence $y \triangleright x \neq x$ for all $x \in g^G$, $y \in h^G$. But $\varphi_y|_{g^G}$ is a transposition for all $y \in h^G$ by Lemma 5.15(4), and hence $|g^G| = 2$.

If $|Y_1| = 1$ then h^G is commutative and $g^G \cup h^G \simeq X_2^{2,2}$ by Lemma 5.17. Suppose next that $|Y_1| = 2$. Then $h^G \simeq X_2^{2,2}$ by Lemma 1.12. Let $h' \in Y_1$ with $h' \neq h$. Since $ghg \triangleright h = h$ by Lemma 5.15(5) and since $hg \triangleright h \neq g \triangleright h$, we conclude that $g^2 \triangleright h \neq h$, $\varphi_g = (h\, g \triangleright h\, h'\, g \triangleright h')$, and $\varphi_{h \triangleright g} = \varphi_g^{-1}$. Therefore $g^G \cup h^G \simeq X_4^{4,2}$.

Finally, assume that $|Y_1| = 3$. Let $r_2 \in Y_1$. Then $r_2 \triangleright x \neq x$ for all $x \in Y_2$, by Lemma 1.12. Now take $r_3 \in Y_2 \setminus \{g \triangleright r_2, g^{-1} \triangleright r_2\}$ and $r_1 \in Y_1 \setminus \{r_3 \triangleright r_2, g^{-1} \triangleright r_3\}$. Then $(\operatorname{ad} W)^4(V) \neq 0$ by Corollary 5.10 with $s = g$, a contradiction. □

Lemma 5.22. *Assume that* $h^2 \triangleright g = g$. *Then* $h^2 \triangleright (g \triangleright h) = g \triangleright h$. *In particular,* h^G *is not isomorphic to any of* $(123)^{\mathbb{A}_4}$, $\operatorname{Aff}(5,2)$ *and* $\operatorname{Aff}(5,3)$.

Proof. The first claim follows from the definition of a quandle. Since h and $g \triangleright h$ are fixed points of $\varphi_h^2|_{h^G}$, the second claim follows from Remark 1.6. □

Lemma 5.23. *Assume that* $(\operatorname{ad} V)^2(W) = 0$ *and* $(\operatorname{ad} W)^4(V) = 0$. *Then* h^G *is not isomorphic to* $\operatorname{Aff}(5,4)$.

Proof. Assume that $h^G \simeq \operatorname{Aff}(5,4)$. Then h^G can be generated by two elements x and y, $x \neq y$. By Lemma 5.15(4), $\varphi_x|_{g^G}$ and $\varphi_y|_{g^G}$ are transpositions. By Lemma 5.19, either $|g^G| = 2$ or $|g^G| = 3$, $\varphi_x|_{g^G} \neq \varphi_y|_{g^G}$. Assume the second case. Let $z \in g^G$ such that $x \triangleright z \neq z$, $y \triangleright z \neq z$. Then $x \triangleright z \neq y \triangleright z$, $x \triangleright (y \triangleright z) = y \triangleright z$, $y \triangleright (x \triangleright z) = x \triangleright z$. Therefore

$$xyxyx \triangleright z = y \triangleright z \neq x \triangleright z = yxyxy \triangleright z,$$

a contradiction to $xyxyx = yxyxy$ in G. Hence $|g^G| = 2$.

Now $g \triangleright z \neq z$ for all $z \in h^G$ and therefore we may assume that $g^3 \triangleright h \neq h$. Moreover, for all $z_1, z_2 \in h^G$ there exists $z \in h^G$ such that $z \triangleright z_1 = z_2$. So let $r_2 \in h^G$ such that $r_2 \triangleright h = g \triangleright h$ and let $r_3 = h$. Since $ghgh = hghg$ by Lemma 5.15(5), we conclude that $r_2 \triangleright r_3 \neq r_3$, $g \triangleright r_2 \neq r_2$, $g \triangleright r_2 \neq r_3$ since

$$(g \triangleright r_2) \triangleright (g \triangleright h) = g \triangleright (r_2 \triangleright h) = g^2 \triangleright h \neq g^{-1} \triangleright h = h \triangleright (g \triangleright h),$$

$g \triangleright r_3 \notin \{r_2, r_3\}$. Moreover, $r_3 r_2 \triangleright r_3 = hg \triangleright h = g^{-1} \triangleright r_3$, and hence there exists $r_1 \in h^G \setminus \{r_3 r_2 \triangleright r_3, r_3 \triangleright r_2, r_3, g^{-1} \triangleright r_2, g^{-1} \triangleright r_3\}$. Since $r_1 \triangleright g \neq g$, Corollary 5.10 with $s = g$ implies that $(\operatorname{ad} W)^4(V) \neq 0$. This is a contradiction and hence $h^G \not\simeq \operatorname{Aff}(5,4)$. □

Lemma 5.24. *Assume that* $(\operatorname{ad} V)^2(W) = 0$ *and* $(\operatorname{ad} W)^4(V) = 0$. *Then* h^G *is neither isomorphic to* $(1234)^{\mathbb{S}_4}$ *nor to* $(12)^{\mathbb{S}_4}$.

Proof. Assume that $h^G \simeq (1234)^{\mathbb{S}_4}$ or $h^G \simeq (12)^{\mathbb{S}_4}$. Let $r_3 \in h^G$, $s \in g^G$ with $s \triangleright r_3 \neq r_3$ and let $x \in h^G \setminus \{r_3\}$ with $r_3 \triangleright x = x$. It suffices to show that $s \triangleright r_3 = x$, $s \triangleright x = r_3$, and $\varphi_s|_{h^G} \neq (x\, r_3)$. Indeed, let $r_2 \in h^G \setminus \{r_3, x\}$ with

$s \triangleright r_2 \neq r_2$ and let $r_1 \in h^G \setminus \{r_3 r_2 \triangleright r_3, r_3 \triangleright r_2, r_3, s^{-1} \triangleright r_3, s^{-1} \triangleright r_2\}$. Then $r_1 \triangleright r_3 \neq r_3$ since $r_1 \neq r_3$ and $r_1 \neq s^{-1} \triangleright r_3 = x$, and hence Corollary 5.10 contradicts to $(\operatorname{ad} W)^4(V) = 0$.

Now we show that $s \triangleright r_3 = x$, $s \triangleright x = r_3$. First, $\varphi_{r_3}|_{g^G}$ and $\varphi_x|_{g^G}$ are transpositions by Lemma 5.15(4). If $h^G \simeq (1234)^{\mathbb{S}_4}$ then $r_3^2 \triangleright (s \triangleright r_3) = s \triangleright r_3$ and $\varphi_{r_3}^2|_{h^G}$ has only r_3 and x as fixed points. Hence $s \triangleright r_3 = x$ and similarly $s \triangleright x = r_3$. If $h^G \simeq (12)^{\mathbb{S}_4}$ then Lemma 5.18 implies that $\varphi_{r_3}|_{g^G} = \varphi_x|_{g^G}$. Hence $r_3 x \triangleright (s \triangleright r_3) = s \triangleright r_3$. Since $\varphi_{r_3}\varphi_x|_{h^G}$ has only r_3 and x as fixed points, we conclude that $s \triangleright r_3 = x$ and similarly $s \triangleright x = r_3$.

Now we show that there exists $y \in h^G \setminus \{r_3, x\}$ such that $s \triangleright y \neq y$. If $h^G \simeq (1234)^{\mathbb{S}_4}$ then Lemma 5.19 implies that $|g^G| \leq 3$ and the claim holds. If $h^G \simeq (12)^{\mathbb{S}_4}$ then let $z \in h^G \setminus \{r_3, x\}$. Then r_3, x and z generate h^G as a quandle. Recall that $\varphi_{r_3}|_{g^G} = \varphi_x|_{g^G} = (s\, x \triangleright s)$. If $\varphi_z|_{g^G} = (a\, b)$ with $|\{s, x \triangleright s, a, b\}| = 4$ then $|g^G| = 2$ by a calculation similar to (5.9) of Lemma 5.19, a contradiction. Otherwise $|g^G| \leq 3$ as in the proof of Lemma 5.19. Then again $y \triangleright s \neq s$ for four or six elements $y \in h^G$. $\square$

Proposition 5.25. *Assume that* $(\operatorname{ad} V)^2(W) = 0$ *and* $(\operatorname{ad} W)^4(V) = 0$. *Then* $g^G \cup h^G$ *is isomorphic to* $X_2^{2,2}$, $X_3^{3,2}$ *or* $X_4^{4,2}$.

Proof. First, $g^G \neq h^G$ by Lemma 5.15(2). If h^G is commutative then $X \simeq X_2^{2,2}$ by Lemma 5.17. If h^G is decomposable then $X \simeq X_2^{2,2}$ or $X \simeq X_4^{4,2}$ by Lemma 5.21. Finally, suppose that h^G is non-commutative and indecomposable. Then Corollary 5.11 implies that h^G is isomorphic to one of the non-commutative quandles of (5.8). Since $h^2 \triangleright g = g$ by Lemma 5.15(5), Lemmas 5.22, 5.23, and 5.24 imply that $h^G \simeq (12)^{\mathbb{S}_3}$. Then $|g^G| = 2$ or $|g^G| = 3$ by Lemma 5.19 and g^G is commutative by Lemma 5.15(1). If $|g^G| = 2$ then $g \triangleright x \neq x$ for all $x \in h^G$ and hence φ_g is a three-cycle and $\varphi_{h \triangleright g} = \varphi_h \varphi_g \varphi_h^{-1} = \varphi_g^{-1}$. Thus $X \simeq X_3^{3,2}$. If $|g^G| = 3$ then $(g \triangleright h) \triangleright g = g \triangleright (h \triangleright g) = h \triangleright g$. Then Lemma 5.15(4) implies that $\varphi_{g \triangleright h}|_{g^G} = \varphi_h|_{g^G} = (g\, h \triangleright g)$, a contradiction to Lemma 5.19 and $|g^G| = 3$. $\square$

5.4. **The proof of Theorem 4.4.** Let $g \in \operatorname{supp} V$, $h \in \operatorname{supp} W$. Then $\operatorname{supp} V = g^G$, $\operatorname{supp} W = h^G$ by assumption. Let $X = g^G \cup h^G$. If g^G and h^G commute then $X \simeq X_3^{3,1}$ or $X \simeq X_T^{4,1}$ by Proposition 5.14. Otherwise, g^G and h^G do not commute and $X \simeq X_2^{2,2}$ or $X \simeq X_4^{4,2}$ or $X \simeq X_3^{3,2}$ by Proposition 5.25. The enveloping groups of the quandles $X_T^{4,1}$, $X_2^{2,2}$, $X_3^{3,1}$, $X_3^{3,2}$ and $X_4^{4,2}$ were computed in §2. Hence the theorem follows from the universal property of the enveloping group, see Remark 1.7. $\square$

References

[1] N. Andruskiewitsch, F. Fantino, M. Graña, and L. Vendramin. Finite-dimensional pointed Hopf algebras with alternating groups are trivial. *Ann. Mat. Pura Appl. (4)*, 190(2):225–245, 2011.

[2] N. Andruskiewitsch, F. Fantino, M. Graña, and L. Vendramin. Pointed Hopf algebras over the sporadic simple groups. *J. Algebra*, 325:305–320, 2011.
[3] N. Andruskiewitsch and M. Graña. From racks to pointed Hopf algebras. *Adv. Math.*, 178(2):177–243, 2003.
[4] N. Andruskiewitsch, I. Heckenberger, and H.-J. Schneider. The Nichols algebra of a semisimple Yetter-Drinfeld module. *Amer. J. Math.*, 132(6):1493–1547, 2010.
[5] N. Andruskiewitsch and H.-J. Schneider. Lifting of quantum linear spaces and pointed Hopf algebras of order p^3. *J. Algebra*, 209(2):658–691, 1998.
[6] N. Andruskiewitsch and H.-J. Schneider. Finite quantum groups and Cartan matrices. *Adv. Math.*, 154(1):1–45, 2000.
[7] N. Andruskiewitsch and H.-J. Schneider. On the classification of finite-dimensional pointed Hopf algebras. *Ann. of Math. (2)*, 171(1):375–417, 2010.
[8] I. Angiono. A presentation by generators and relations of Nichols algebras of diagonal type and convex orders on root systems. *Accepted for publication in J. Europ. Math. Soc., arXiv:1008.4144*.
[9] I. Angiono. On Nichols algebras of diagonal type. *Accepted for publication in J. Reine Angew. Math., arXiv:1104.0268*.
[10] M. Cuntz and I. Heckenberger. Weyl groupoids of rank two and continued fractions. *Algebra Number Theory*, 3(3):317–340, 2009.
[11] M. Graña, I. Heckenberger, and L. Vendramin. Nichols algebras of group type with many quadratic relations. *Adv. Math.*, 227(5):1956–1989, 2011.
[12] P. Hall. The classification of prime-power groups. *J. Reine Angew. Math.*, 182:130–141, 1940.
[13] I. Heckenberger. The Weyl groupoid of a Nichols algebra of diagonal type. *Invent. Math.*, 164(1):175–188, 2006.
[14] I. Heckenberger. Classification of arithmetic root systems. *Adv. Math.*, 220(1):59–124, 2009.
[15] I. Heckenberger and H.-J. Schneider. Nichols algebras over groups with finite root system of rank two I. *J. Algebra*, 324(11):3090–3114, 2010.
[16] I. Heckenberger and H.-J. Schneider. Root systems and Weyl groupoids for Nichols algebras. *Proc. Lond. Math. Soc. (3)*, 101(3):623–654, 2010.
[17] I. Heckenberger and H. Yamane. A generalization of Coxeter groups, root systems, and Matsumoto's theorem. *Math. Z.*, 259(2):255–276, 2008.
[18] V. K. Kharchenko. A quantum analogue of the Poincaré-Birkhoff-Witt theorem. *Algebra Log.*, 38(4):476–507, 509, 1999.
[19] G. Lusztig. *Introduction to quantum groups*. Modern Birkhäuser Classics. Birkhäuser/Springer, New York, 2010. Reprint of the 1994 edition.
[20] D. M. Rocke. p-groups with abelian centralizers. *Proc. London Math. Soc. (3)*, 30:55–75, 1975.
[21] M. Rosso. Quantum groups and quantum shuffles. *Invent. Math.*, 133(2):399–416, 1998.

Philipps-Universität Marburg, FB Mathematik und Informatik, Hans-Meerwein-Strasse, 35032 Marburg, Germany

E-mail address: `heckenberger@mathematik.uni-marburg.de`

E-mail address: `lvendramin@dm.uba.ar`